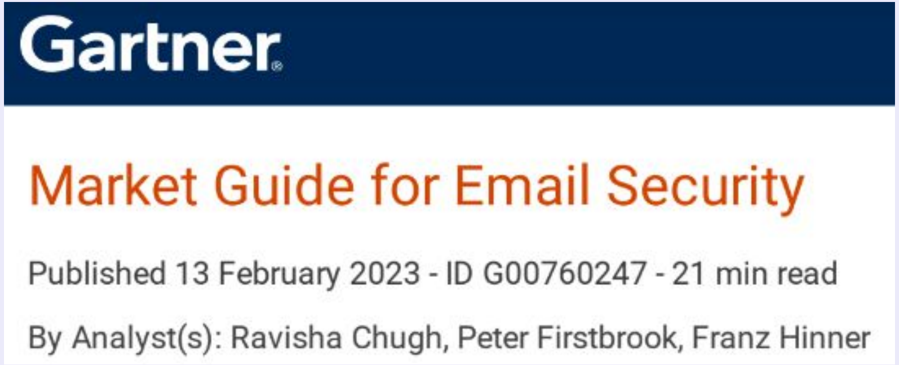
Abnormal

Minimising user exposure to threats

Tim Bentley



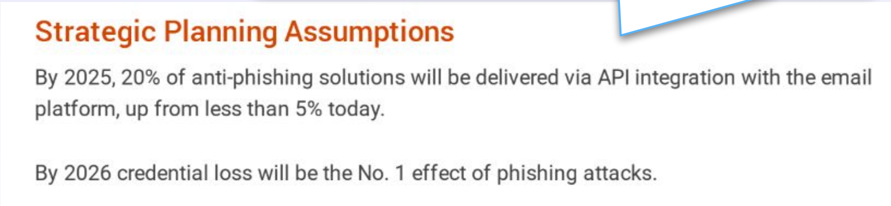
Gartner

Market Guide for Email Security

Published 13 February 2023 - ID G00760247 - 21 min read

By Analyst(s): Ravisha Chugh, Peter Firstbrook, Franz Hinner

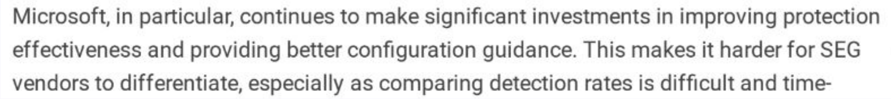
- Mass adoption of ICES
- Continued growth of credential phish



Strategic Planning Assumptions

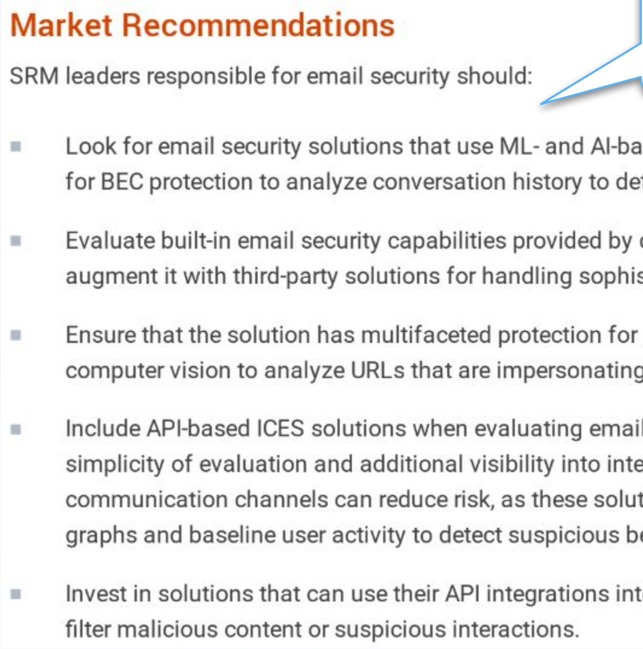
By 2025, 20% of anti-phishing solutions will be delivered via API integration with the email platform, up from less than 5% today.

By 2026 credential loss will be the No. 1 effect of phishing attacks.



Microsoft, in particular, continues to make significant investments in improving protection effectiveness and providing better configuration guidance. This makes it harder for SEG vendors to differentiate, especially as comparing detection rates is difficult and time-

- Closer parity between Native Controls and SEGs



Market Recommendations

SRM leaders responsible for email security should:

- Look for email security solutions that use ML- and AI-based anti-phishing technology for BEC protection to analyze conversation history to detect anomalies.
- Evaluate built-in email security capabilities provided by cloud email systems and augment it with third-party solutions for handling sophisticated attacks.
- Ensure that the solution has multifaceted protection for credential theft, as well as computer vision to analyze URLs that are impersonating common log-on pages.
- Include API-based ICES solutions when evaluating email security solutions. The simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, as these solutions create communication graphs and baseline user activity to detect suspicious behavior.
- Invest in solutions that can use their API integrations into collaboration platforms to filter malicious content or suspicious interactions.

- AI and ML
- API based

Microsoft recommend Abnormal Security

“Abnormal Security augments native Microsoft security services (Azure Sentinel, Defender for Office 365) to protect our mutual customers from advanced socially-engineered attacks while also reducing security stack complexity and improving SOC efficiency”

Member of
Microsoft Intelligent
Security Association
Microsoft

Member Of The Microsoft Intelligent Security Association

The Microsoft Intelligent Security Association (MISA) is an ecosystem of independent software vendors and managed security service providers that have integrated their solutions to better defend against a world of increasing threats. MISA members are top experts from across the cybersecurity industry with the shared goal of improving customer security.

Microsoft Preferred Solution

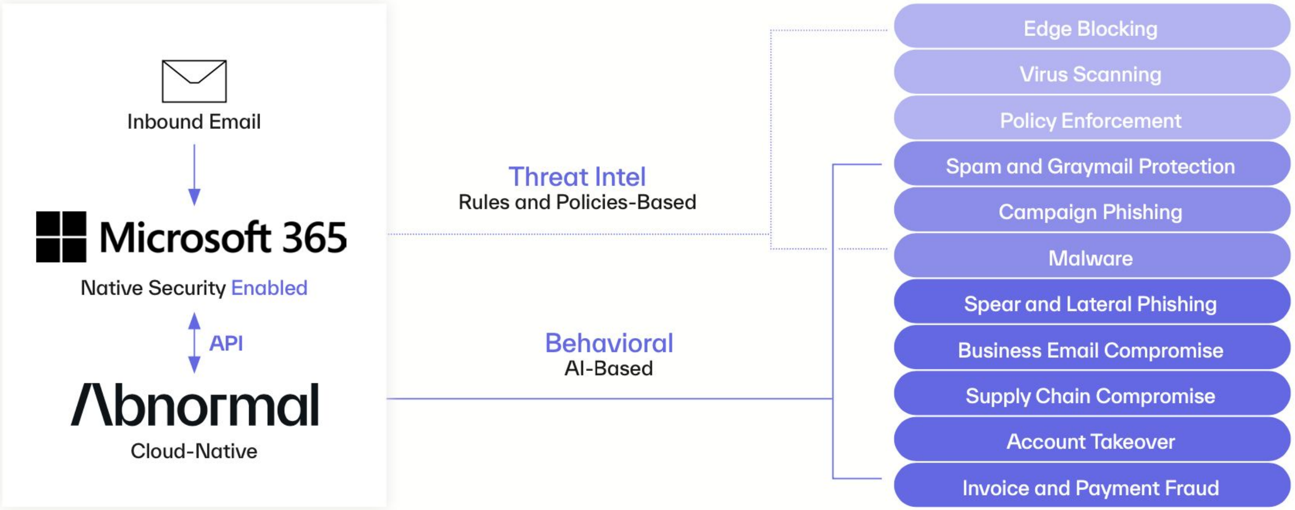
Preferred solutions are selected by a team of Microsoft experts and are published by Microsoft partners with deep, proven expertise and capabilities to address specific customer needs in a category, industry, or industry vertical.

Member Of The Microsoft AI Inner Circle Partner Program

The AI Inner Circle Partner program is designed for partners who provide custom services or enhanced AI product solutions utilizing Microsoft AI technologies. This program recognizes a partner's unique expertise in specific industries and their ability to drive business transformation using the power of AI and data.

abnormalsecurity.com/microsoft-partnership

Working in harmony with Microsoft



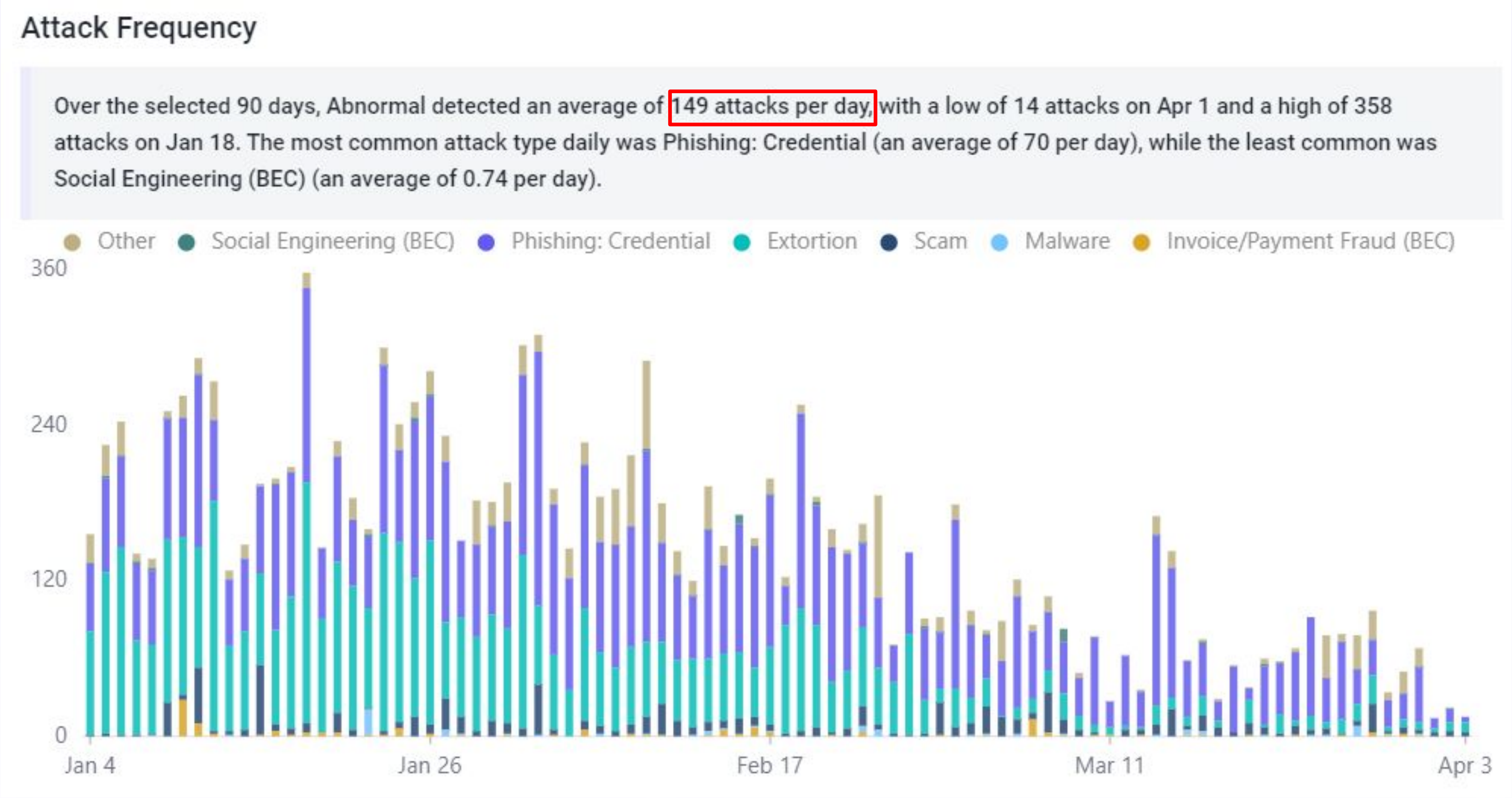
Benefits

Prevents all email attacks with high efficacy.

Simplifies email security.

Streamlines operations to increase productivity.

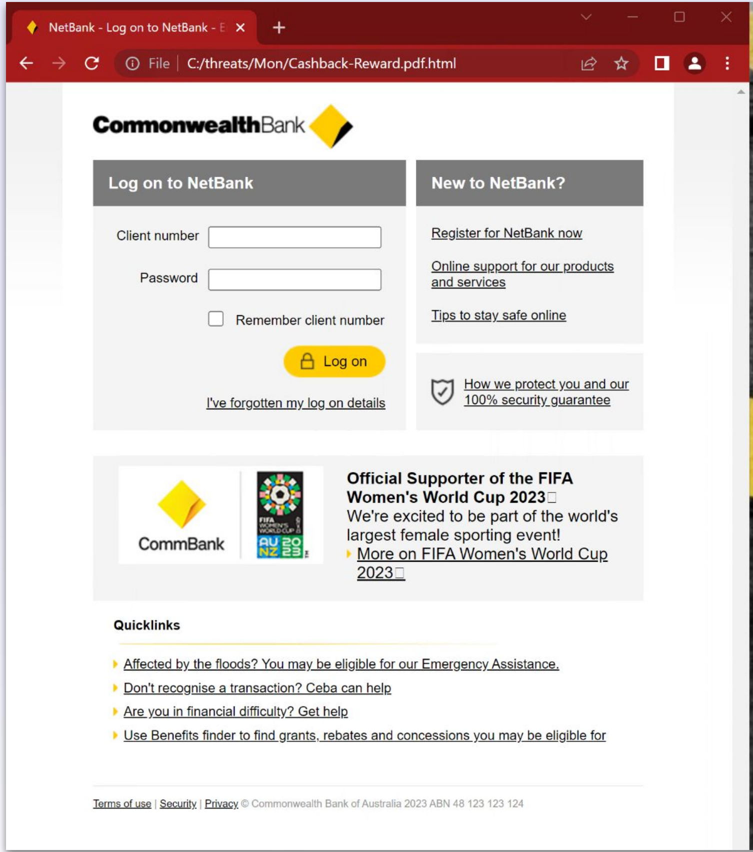
Australian customer - behind Proofpoint



Attack Frequency

Over the selected 90 days, Abnormal detected an average of 149 attacks per day, with a low of 14 attacks on Apr 1 and a high of 358 attacks on Jan 18. The most common attack type daily was Phishing: Credential (an average of 70 per day), while the least common was Social Engineering (BEC) (an average of 0.74 per day).

Which one is fake?


NetBank - Log on to NetBank - E
File

C:/threats/Mon/Cashback-Reward.pdf.html

CommonwealthBank

Log on to NetBank

Client number

Password

□ Remember client number

Log on

I've forgotten my log on details

New to NetBank?

Register for NetBank now

Online support for our products and services

Tips to stay safe online

How we protect you and our 100% security guarantee

CommBank
FIFA WOMEN'S WORLD CUP AU NZ 2023

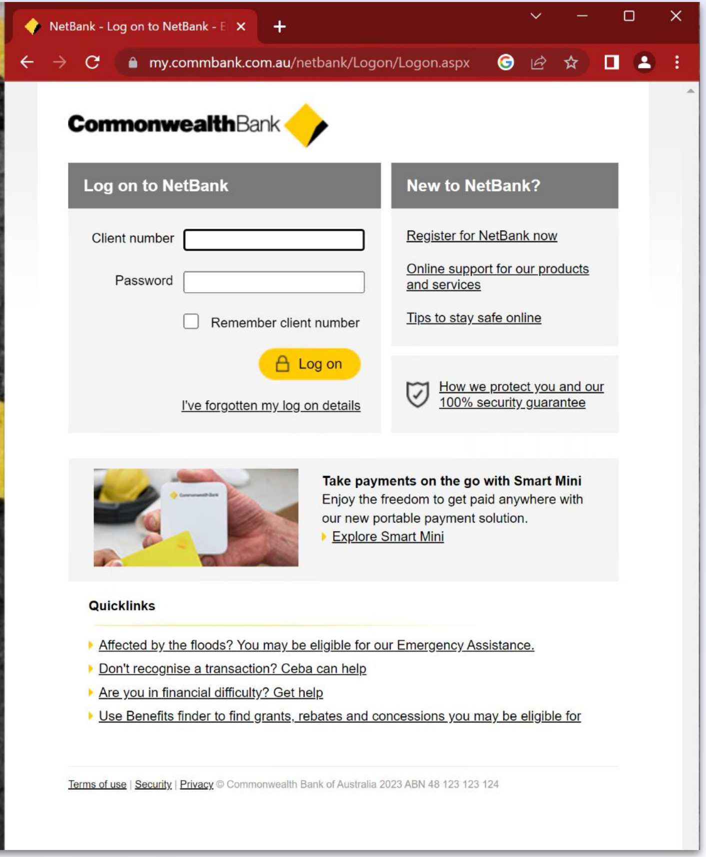
Official Supporter of the FIFA Women's World Cup 2023□
We're excited to be part of the world's largest female sporting event!

- More on FIFA Women's World Cup 2023□

Quicklinks

- Affected by the floods? You may be eligible for our Emergency Assistance.
- Don't recognise a transaction? Ceba can help
- Are you in financial difficulty? Get help
- Use Benefits finder to find grants, rebates and concessions you may be eligible for

Terms of use | Security | Privacy © Commonwealth Bank of Australia 2023 ABN 48 123 123 124



my.commbank.com.au/netbank/Logon/Logon.aspx

CommonwealthBank

Log on to NetBank

Client number

Password

□ Remember client number

Log on

I've forgotten my log on details

New to NetBank?

Register for NetBank now

Online support for our products and services

Tips to stay safe online

How we protect you and our 100% security guarantee

Take payments on the go with Smart Mini
Enjoy the freedom to get paid anywhere with our new portable payment solution.

- Explore Smart Mini

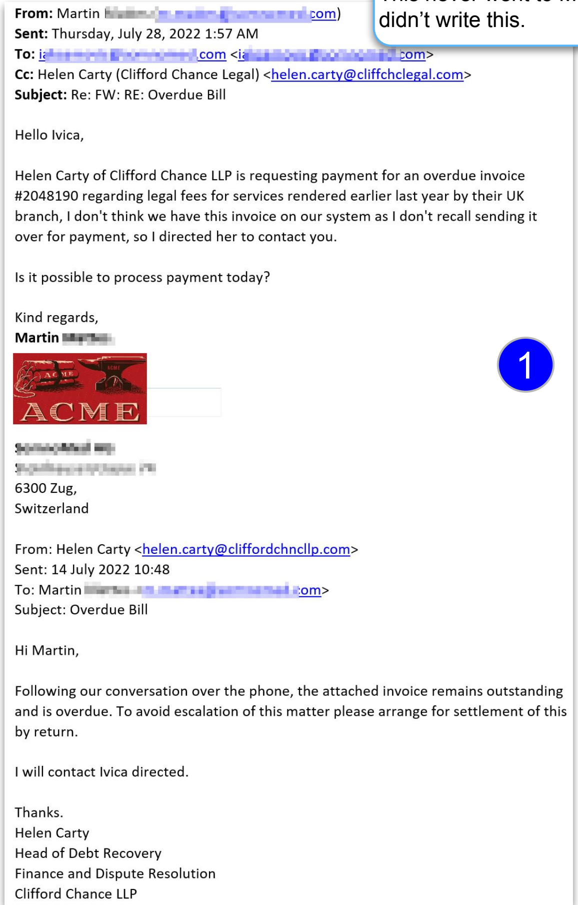
Quicklinks

- Affected by the floods? You may be eligible for our Emergency Assistance.
- Don't recognise a transaction? Ceba can help
- Are you in financial difficulty? Get help
- Use Benefits finder to find grants, rebates and concessions you may be eligible for

Terms of use | Security | Privacy © Commonwealth Bank of Australia 2023 ABN 48 123 123 124

Advanced Australian invoice fraud

Fake thread on the bottom of the email. This never went to Martin and Martin didn't write this.



From: Martin [redacted]com)
Sent: Thursday, July 28, 2022 1:57 AM
To: i[redacted].com <i[redacted].com>
Cc: Helen Carty (Clifford Chance Legal) <helen.carty@cliffchclegal.com>
Subject: Re: FW: RE: Overdue Bill

Hello Ivica,

Helen Carty of Clifford Chance LLP is requesting payment for an overdue invoice #2048190 regarding legal fees for services rendered earlier last year by their UK branch, I don't think we have this invoice on our system as I don't recall sending it over for payment, so I directed her to contact you.

Is it possible to process payment today?

Kind regards,
Martin [redacted]

[redacted]
6300 Zug,
Switzerland

From: Helen Carty <helen.carty@cliffordchncllp.com>
Sent: 14 July 2022 10:48
To: Martin [redacted]om>
Subject: Overdue Bill

Hi Martin,

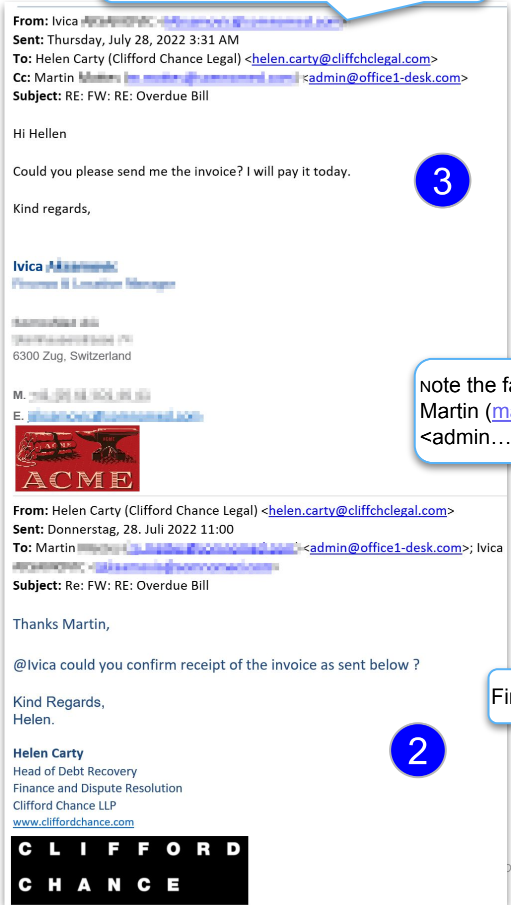
Following our conversation over the phone, the attached invoice remains outstanding and is overdue. To avoid escalation of this matter please arrange for settlement of this by return.

I will contact Ivica directed.

Thanks.
Helen Carty
Head of Debt Recovery
Finance and Dispute Resolution
Clifford Chance LLP

1

Ivica from Acme replies to threat-actor (Clifford Chance impersonator)



From: Ivica [redacted]
Sent: Thursday, July 28, 2022 3:31 AM
To: Helen Carty (Clifford Chance Legal) <helen.carty@cliffchclegal.com>
Cc: Martin [redacted] <admin@office1-desk.com>
Subject: RE: FW: RE: Overdue Bill

Hi Hellen

Could you please send me the invoice? I will pay it today.

Kind regards,

Ivica [redacted]

[redacted]
6300 Zug, Switzerland

M. [redacted]
E. [redacted]

From: Helen Carty (Clifford Chance Legal) <helen.carty@cliffchclegal.com>
Sent: Donnerstag, 28. Juli 2022 11:00
To: Martin [redacted] <admin@office1-desk.com>; Ivica [redacted]
Subject: Re: FW: RE: Overdue Bill

Thanks Martin,

@Ivica could you confirm receipt of the invoice as sent below ?

Kind Regards,
Helen.

Helen Carty
Head of Debt Recovery
Finance and Dispute Resolution
Clifford Chance LLP
www.cliffordchance.com

CLIFFORD
CHANCE

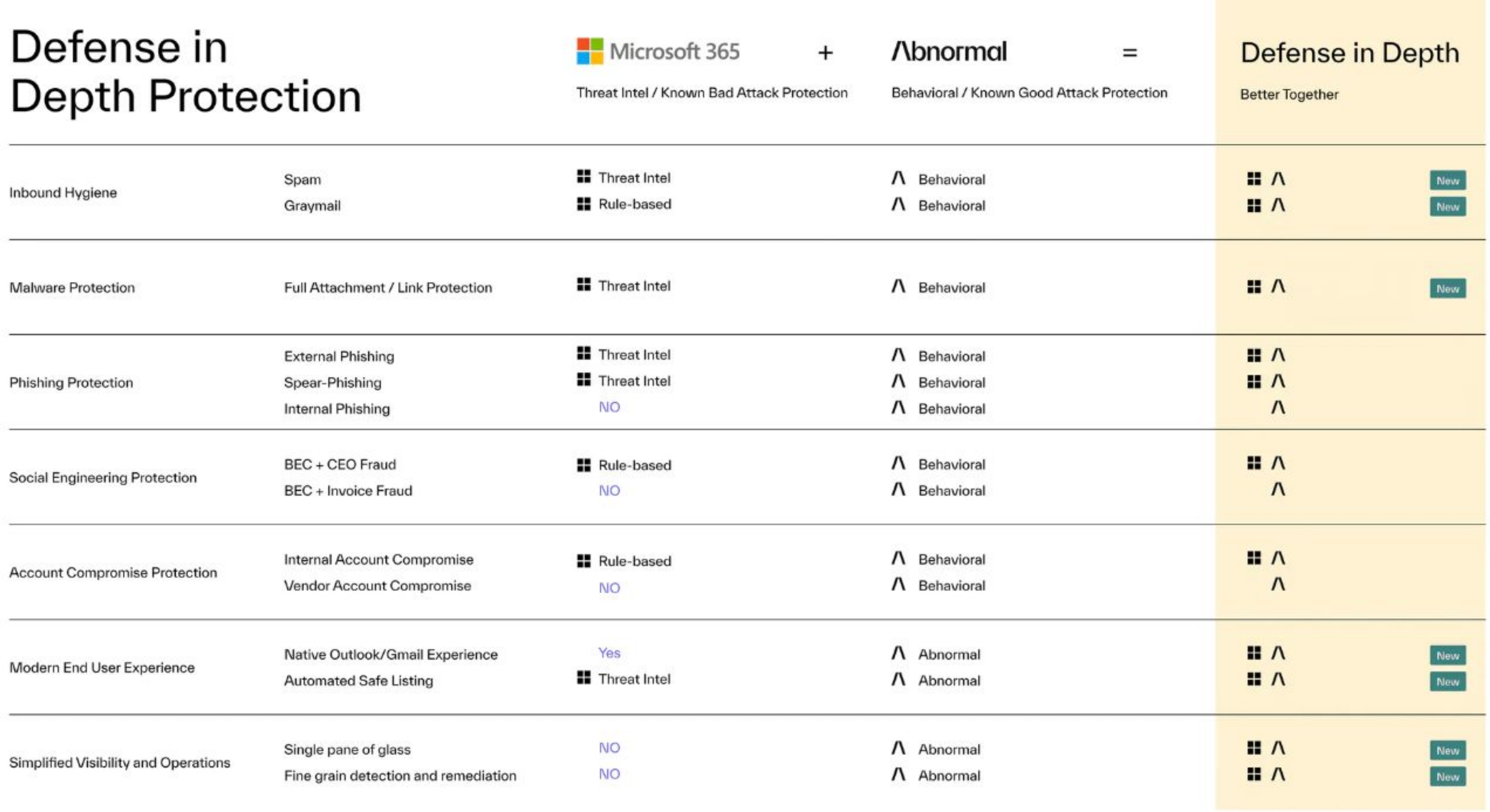
3

Note the fake Cc:
Martin (martin.surname@acme.com) <admin…

First email to Ivica at Acme

2

Working in harmony with Microsoft



Defense in Depth Protection		Microsoft 365 + Threat Intel / Known Bad Attack Protection	Abnormal = Behavioral / Known Good Attack Protection	Defense in Depth Better Together	
Inbound Hygiene	Spam	⊞ Threat Intel	Λ Behavioral	⊞ Λ	New
	Graymail	⊞ Rule-based	Λ Behavioral	⊞ Λ	New
Malware Protection	Full Attachment / Link Protection	⊞ Threat Intel	Λ Behavioral	⊞ Λ	New
Phishing Protection	External Phishing	⊞ Threat Intel	Λ Behavioral	⊞ Λ	
	Spear-Phishing	⊞ Threat Intel	Λ Behavioral	⊞ Λ	
	Internal Phishing	NO	Λ Behavioral	Λ	
Social Engineering Protection	BEC + CEO Fraud	⊞ Rule-based	Λ Behavioral	⊞ Λ	
	BEC + Invoice Fraud	NO	Λ Behavioral	Λ	
Account Compromise Protection	Internal Account Compromise	⊞ Rule-based	Λ Behavioral	⊞ Λ	
	Vendor Account Compromise	NO	Λ Behavioral	Λ	
Modern End User Experience	Native Outlook/Gmail Experience	Yes	Λ Abnormal	⊞ Λ	New
	Automated Safe Listing	⊞ Threat Intel	Λ Abnormal	⊞ Λ	New
Simplified Visibility and Operations	Single pane of glass	NO	Λ Abnormal	⊞ Λ	New
	Fine grain detection and remediation	NO	Λ Abnormal	⊞ Λ	New

abnormalsecurity.com/microsoft-partnership